



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 29 June 2005

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The Washington Post reports the Virginia Railway Express is enforcing CSX speed reductions, meant to keep tracks from overheating and developing dangerous kinks during extreme summer heat days. (See item [7](#))
- The Associated Press reports the World Health Organization has appealed to China to test migratory geese and gulls for avian flu in a western region, warning that they might spread the virus when they fly south this summer. (See item [18](#))
- The Center for Infectious Disease Research & Policy News reports there is a momentum building for cell–culture flu vaccines as opposed to the traditional egg–based method. (See item [19](#))

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS/IAIP Products & Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *June 28, Reuters* — **France to host world's first nuclear fusion plant.** Science's quest to find a cheap and inexhaustible way to meet global energy needs took a major step forward on Tuesday, June 28, when the 30–nation consortium International Thermonuclear Experimental Reactor (ITER) chose France to host the world's first nuclear fusion reactor. After months of wrangling, France defeated a bid from Japan and signed a deal to site the \$12.18 billion

experimental reactor in Cadarache, near Marseille. The project will seek to turn seawater into fuel by mimicking the way the sun produces energy. Its backers say it would be cleaner than existing nuclear reactors, but critics argue it could be at least 50 years before a commercially viable reactor is built, if at all. Unlike existing fission reactors, which release energy by splitting atoms apart, ITER would generate energy by combining them. Power has been harnessed from fusion in laboratories but scientists have so far been unable to build a commercially viable reactor, despite decades of research. The 500 megawatt ITER reactor will use deuterium, extracted from seawater, as its major fuel and a giant electromagnetic ring to fuse atomic nuclei at extremely high temperatures.

Source: http://news.yahoo.com/news?tmpl=story&u=/nm/20050628/sc_nm/energy_france_nuclear_dc_5

2. *June 28, Associated Press* — **Cable failure caused substation fire in Chicago.** Failure of an underground transmission cable caused a fire and led to a power outage that affected thousands of homes and businesses, according to an initial Commonwealth Edison (ComEd) investigation announced Tuesday, June 28. The cable failure Friday, June 24, at a substation on Chicago's west side was not related to the city's heat wave, ComEd said. None of the lines was loaded above capacity and the fire started at about 8:40 p.m., after the day's power usage had peaked. Coolant fluid caught fire when the transmission cable failed. The fire damaged six of the 12 transmission cables housed in the service tunnel where the fire occurred, according to ComEd. The outage affected 51,000 customers. Most got their electricity restored within three hours, but several thousand had to wait until the following afternoon or evening before the lights came back on.

Source: <http://www.suntimes.com/output/news/comed28.html>

3. *June 28, Times Argus (VT)* — **High temperatures and equipment malfunction test Vermont's transmission system.** This week's heat wave may drive power usage in Vermont to an all-time summer high, according to officials at the Vermont Electric Power Company (VELCO). VELCO president and CEO John Donleavy said the utility expected that the peak on Monday, June 27, would surpass the previous summertime peak of 1,022.7 megawatts set on August 15, 2002. The announcement by VELCO, the state's transmission utility, also came on a day when a key piece of equipment failed temporarily at one of the company's substations, placing parts of the system in jeopardy for several hours. At 3:50 a.m. on Monday the utility experienced an equipment failure at its Granite substation. Crews were dispatched to the substation and began testing a breaker and a transformer at the substation. During this time the substation's connection to a 230-kilovolt (kV) line that feeds electricity into Vermont from New Hampshire was broken. That resulted in a temporary disruption of a line carrying between 80 and 100 megawatts to the Vermont system. The loss of this source of power, coupled with extremely high demand owing to the extended heat wave, put parts of VELCO's transmission system at risk, Donleavy said.

Source: <http://www.timesargus.com/apps/pbcs.dll/article?AID=/20050628/NEWS/506280324/1003>

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report.

[\[Return to top\]](#)

Banking and Finance Sector

4. *June 28, IDG News Service* — **Online scammers get jail sentences.** Two men have been sentenced to a total of 10 years in prison for their roles in a wide range of online fraud activities in the United Kingdom. Douglas Harvard, a U.S. citizen, was arrested by the National Hi-Tech Crime Unit (NHTCU) in Leeds earlier this month following an investigation into Eastern European crime syndicates. Police found documents, correspondence and equipment for creating false identities, as well as evidence that he was being assisted by a second man, British citizen Lee Elwood. Elwood, who is based in Glasgow, was arrested a few days later and charged with conspiracy to defraud after police found a large quantity of forged bank documents, credit card holograms, computers and other equipment. The pair's extensive online fraud activities led authorities to warn about the growing rate of cybercrime. Both men were heavily involved in websites that promoted and facilitated a range of criminal activities, according to the NHTCU. Both men were moderators on the Cardplanet and Shadowcrew Websites, which gave them the ability to monitor, approve and post articles to newsgroups. Once the suspects contacted each other over the Internet, they exchanged stolen information and counterfeit documents, authorities said.

Source: [http://www.techworld.com/security/news/index.cfm?NewsID=3938
&Page=1&pagePos=2](http://www.techworld.com/security/news/index.cfm?NewsID=3938&Page=1&pagePos=2)

[\[Return to top\]](#)

Transportation and Border Security Sector

5. *June 28, Government Accountability Office* — **GAO-05-674: Public Transportation: Opportunities Exist to Improve the Communication and Transparency of Changes Made to the New Starts Process (Report).** The Transportation Equity Act for the 21st Century (TEA-21) and subsequent legislation authorized about \$13.5 billion in guaranteed funding for the Federal Transit Administration's (FTA) New Starts program, which is used to select fixed guide way transit projects, such as rail and trolley projects, and to award full funding grant agreements (FFGA). The Government Accountability Office (GAO) assessed the New Starts process for the fiscal year 2006 cycle. GAO identified (1) the number of projects that were evaluated, rated, and proposed for new FFGAs and the proposed funding commitments in the administration's budget request; (2) changes FTA has made to the New Starts application, evaluation, rating, and oversight processes since the fiscal year 2001 evaluation cycle and how these changes have been communicated to project sponsors; and (3) how FTA developed the measures used to evaluate and rate projects from the criteria outlined in TEA-21 and how those measures are used in the rating process. This report makes a number of recommendations

intended to ensure that the New Starts regulations reflect FTA's current evaluation and rating process and ensure that FTA's New Starts evaluation process and policies are objective, transparent, and follow the spirit of federal statutes and regulations. FTA officials agreed with the findings and recommendations in this report.

Highlights: <http://www.gao.gov/highlights/d05674high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-05-674>

6. *June 28, Associated Press* — **Minuteman New Mexico patrols to start in October.** The Minuteman Civil Defense Corps, made up of civilian volunteers, will officially begin its patrols of the southern New Mexico border in October. New Mexico Minuteman chapter director Bob Wright said he received a generally positive response from people who attended a town hall meeting in Columbus, NM, on Sunday, June 26. Several Columbus residents in the audience of about 80 said they support the group's plans to deploy its civilian patrols around the Columbus area to report, but not detain or confront, suspected illegal immigrants or drug traffickers to authorities. The group drew national attention when it began similar patrols in Arizona in April. The Minuteman Civil Defense corps also will try to deploy volunteers along the Canadian border.

Source: <http://www.sierratimes.com/05/06/28/minuteman.htm>

7. *June 28, Washington Post* — **Virginia Railway Express riders calmly tolerate heat delays.** For commuters on the Virginia Railway Express (VRE), summer means "heat restrictions," or speed reductions meant to keep track from overheating and developing dangerous kinks. VRE trains are staffed by Amtrak and run on tracks owned by CSX Corp., which has imposed the heat delays on passenger trains since 2002 after a heat kink caused an Amtrak derailment in Kensington, MD, CSX spokesperson Misty Skipper said. Heat delays kick in at temperatures around 90 degrees, but Mark Roeber, a spokesperson for the railway, said that this season, the threshold was lowered to 85. Regional engineers have some discretion on that. CSX has some of the strictest heat delay rules in the country, and its directive affects commuters from Florida to Virginia to Maryland. But the epicenter of trouble this season seems to be VRE's Fredericksburg line, where the on-time performance this month has been 52 percent, compared with 90 percent for riders on the Manassas line, where Norfolk Southern owns most of the track. Most riders have a resigned attitude, grateful not to be sitting in traffic on the congested interstate highways.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2005/06/27/AR2005062701571.html>

8. *June 28, Associated Press* — **Newark airport screeners have better than 97% pass rate.** Security screeners at Newark Liberty International Airport are among the best in the nation when it comes to passing annual tests on checkpoint and bomb-detection machine procedures, according to the Transportation Security Administration (TSA). More than 97% of the 1,234 screeners passed the tests, which were given between October and April; TSA said 32 screeners who twice failed exams on the procedures were either fired or allowed to resign. Newark's pass rate is among the highest of the nation's 30 largest commercial airports and better than the airport did last year, said Marcus Arroyo, TSA security director Newark Liberty International.

Source: http://www.usatoday.com/travel/news/2005-06-27-newark-screeners_x.htm

9.

June 28, Associated Press — **United reports \$93M loss on fuel costs.** United Airlines' parent company UAL Corp. said Tuesday, June 28, it had an operating loss of \$21 million for the month, blaming the deficit mostly on fuel expenses that exceeded the May 2004 total by \$93 million. Had fuel costs remained unchanged, the company would have broken even for the month on a net basis. United CEO Glenn Tilton said that the airline is on target to emerge from Chapter 11 bankruptcy this fall and predicted it would turn a profit in 2006. But it's been five years since the Elk Grove Village, IL–based company last made money, and that trend shows no sign of disappearing with oil prices more than 65 percent above year–ago levels. "Fuel is a brutal challenge for our industry," said Jake Brace, United's chief financial officer. "In the face of this challenge, we continue to improve operations across the company, targeting every area of non–labor cost reduction and revenue generation opportunity."

Source: <http://www.fortwayne.com/mld/newssentinel/business/12006093.htm>

[[Return to top](#)]

Postal and Shipping Sector

10. *June 22, DM News* — Postal service net income up over budget. The U.S. Postal Service (USPS) generated net income of \$1.8 billion from October 1 to May 31. USPS net income was \$1.4 billion over budget and revenue totaled \$47.4 billion, which was \$1.1 billion better than planned and up 1.5 percent from the year–ago period. Expenses of \$45.5 billion were \$221.4 million under plan but up four percent from the year–ago period. Total year–to–date mail volume of 142.8 billion pieces was a three percent rise from the year–ago period. The most significant volume increase was in Standard, which jumped 6.1 percent. The category with the next–largest increase was Priority Mail, up 4.2 percent. Other categories producing volume increases in the period included Package Services (2.2 percent), Express Mail (1.6 percent), First Class (0.2 percent) and Periodicals (0.1 percent). The International category declined 0.4 percent.

Source: http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=33150

[[Return to top](#)]

Agriculture Sector

11. *June 28, Science and Development Network* — Genetic shortcut to high–yielding rice. Researchers in China and Japan have combined molecular genetics with traditional plant breeding to create high–yielding rice plants. They say their approach, which greatly reduces the time needed to develop new crop varieties, could be applied to a range of cereal crops and trigger "a new green revolution". The original green revolution of the 1960s developed high–yielding varieties of crops such as rice and wheat by crossing existing strains to find hybrid offspring with desirable traits. It is credited with saving millions of people from starvation. But the success relied on years of painstaking work. "Usually, it takes more than ten years to produce a new variety," says researcher Moto Ashikari.

Source: <http://www.scidev.net/news/index.cfm?fuseaction=readnews&ite mid=2190&language=1>

12. *June 27, The Institute for Genomic Research* — **Genome study of beneficial microbe may help boost plant health.** Scientists have deciphered the genome of a root and seed dwelling bacterium that protects plants from diseases. The research provides clues to better explain how the helpful microbe, *Pseudomonas fluorescens* Pf-5, naturally safeguards roots and seeds from infection by harmful microbes that cause plant diseases. “The genome sequence has helped us identify new chemical pathways that the microbe apparently uses to create what are known as ‘secondary metabolites’ — possibly including new antibiotic compounds,” says Ian Paulsen, who led the sequencing at The Institute for Genomic Research (TIGR), Rockville, MD. The use of naturally occurring, beneficial microbes such as *P. fluorescens* to control plant pathogens is called “biological control.” That method is gaining momentum as a way to grow healthy plants without using synthetic fungicides. Agricultural Research Service pathologist Joyce Loper, an expert on *P. fluorescens* Pf-5, predicts that the new genomic data will help scientists more quickly develop new ways to boost the effectiveness of beneficial microbes in fighting plant diseases.
Source: http://www.tigr.org/new/press_release_06-27-05.shtml
13. *June 27, Associated Press* — **New Mexico deer test positive for chronic wasting disease.** Two mule deer in the Organ Mountains near Las Cruces, NM, have tested positive for chronic wasting disease (CWD) according to the state Department of Game and Fish. The deer were captured as part of an ongoing research project near White Sands Missile Range. There have now been eleven cases of CWD confirmed in New Mexico since 2002, the year a deer found in the foothills of the Organ Mountains tested positive for the disease.
New Mexico Department of Game and Fish Press Release:
http://www.wildlife.state.nm.us/publications/press_releases/documents/0624CWDandcatfish.pdf
Source: <http://espn.go.com/outdoors/hunting/news/2005/0627/2095653.html>
14. *June 27, Agricultural Research Service* — **Pathogen monitoring made easier with paint can shakers.** Stirring, or centrifugation, is a key step by which diagnostic labs genetically identify crop pathogens inhabiting farmers' soils. But shaking, not stirring, the DNA may give farmers more bang for their diagnostic buck, reports George Vandemark, an Agricultural Research Service (ARS) geneticist. Normally, diagnosticians use centrifugation to separate pathogen DNA from other soil sample debris. Polymerase chain reaction and other so-called fingerprinting steps then determine whether the DNA's genetic patterns match those of a particular crop pathogen. The problem is, today's DNA extraction kits only work with 10-gram soil samples. And at around \$15 per test, such extraction can become prohibitive for field-wide surveys — for example, to choose appropriate fungicides or resistant crop varieties, according to Vandemark. His solution was to use paint can shakers, like those used in hardware stores. Instead of paint, though, he modified the shakers to hold test tubes capable of storing 70 grams of soil. To the tubes, he adds small glass beads and a buffer. The beads smash the cells of pathogens in the sample while the buffer protects their escaping DNA from damage by enzymes. After extraction, Vandemark uses PCR-based fingerprinting to determine the pathogen's genetic identity.
Source: <http://www.ars.usda.gov/is/pr/2005/050627.htm>

[[Return to top](#)]

Food Sector

15. *June 28, Ag Professional* — **Cargill purchases properties of Peking University Green Technology.** Cargill has finalized the purchase of part of Peking University Green Technology Co. Ltd. (PGT)'s properties, which includes all the intellectual properties around the production, sales, and marketing of food ingredient systems. The purchase will allow Cargill to leverage PGT's deep customer knowledge and food system expertise to further develop China's food industry and better serve Chinese consumers. A food ingredient system is a blend of different food ingredients, such as emulsifiers and texturizers that provide critical functions, e.g. texture or taste, for a food or beverage product. The food ingredient systems market is an emerging industry in China. China's food market has experienced explosive growth in the past five years. In 2003, China's GDP grew 9.1 percent to \$1.4 trillion while the Chinese food industry achieved a 17.6 percent growth to total \$150 billion. It is expected that the overall food industry in China will likely continue to grow at a pace of more than 10 percent a year in the next five years.
Source: http://www.agprofessional.com/show_story.php?id=33647

[[Return to top](#)]

Water Sector

Nothing to report.

[[Return to top](#)]

Public Health Sector

16. *June 28, Public Library of Science Medicine* — **Development of a new vaccine for the prevention of Lassa fever.** Lassa fever is a disease caused by a virus that is often spread by rodents. The disease is common in parts of West Africa where it causes a significant amount of death and disability among the population. Recently, Lassa fever has been imported by travelers to the United States and Europe. The Lassa virus that causes the disease is also on the list of potential bioweapons agents. Currently, there are no licensed vaccines for Lassa fever, and no experimental vaccine has completely protected nonhuman primates against a lethal challenge. Thomas W. Geisbert, et al generated a replication-competent vaccine against the Lassa virus based on attenuated recombinant vesicular stomatitis virus vectors expressing the Lassa viral glycoprotein. A single intramuscular vaccination of the Lassa vaccine elicited a protective immune response in nonhuman primates against a lethal Lassa virus challenge. No evidence of clinical disease was found in the four monkeys injected with the combination vaccine; they remained healthy. Issues that need to be resolved before the vaccine can be tested in humans include the safety of the vesicular stomatitis carrier virus, how long the vaccine protects after the shot, and whether it is active against different strains of the Lassa virus.
Source: <http://medicine.plosjournals.org/perlserv/?request=get-document&doi=10.1371/journal.pmed.0020183>

17. *June 28, Associated Press* — **Indonesia begins second round of free polio vaccinations.** Indonesia carried out the second round of a massive polio vaccination campaign Tuesday, June

28, as the confirmed number of cases in the country's first brush with the disease in ten years rose to 65. Polio is spread when unvaccinated people come into contact with the feces of those with the virus, often through water. It usually attacks the nervous system, causing paralysis, muscular atrophy, deformation and sometimes death, though only about one in 200 of those infected ever develop symptoms. The 14 new cases occurred in West Java and Banten provinces, close to where the disease was first discovered in April, the World Health Organization (WHO) said in a statement. Last month, about 6.5 million children were vaccinated in West Java, Banten and Jakarta provinces. On Tuesday, women and children flocked to medical centers in those regions for a second dose of the vaccine, a couple of drops of which are squeezed into the mouth of each toddler, the WHO said.

Source: <http://asia.news.yahoo.com/050628/ap/d8b0g6a80.html>

18. *June 28, Associated Press* — **World Health Organization appeals to China to test wild birds for flu, warning migration could spread virus.** The World Health Organization (WHO) appealed to China on Tuesday, June 28, to test migratory geese and gulls for avian flu in a western region where 5,000 birds have died, warning that they might spread the virus when they fly south this summer. Authorities haven't slaughtered the wild birds in remote Qinghai province, as has been done elsewhere to contain the virus, because many are from rare, protected species. Birds around Qinghai Lake, a mating ground for migratory birds, are still dying at a rate of about 20 a day, said Dr. Julie Hall, a World Health Organization expert. Tests showed they died of the H5N1 strain that has killed a total of 54 people in Asia's latest outbreak and prompted the slaughter of millions of chickens and other poultry. The biggest danger could be from birds that are infected but show no symptoms, Hall and other officials said. The birds from Qinghai are likely to head to India and Pakistan in August and September, said Dr. Nouredin Mona, the representative in China for the UN Food and Agriculture Organization. Fortunately, there have been no reports of human cases in the area.

Source: <http://asia.news.yahoo.com/050628/ap/d8b0jpc80.html>

19. *June 27, Center for Infectious Disease Research & Policy News* — **Momentum builds for cell-culture flu vaccines.** Departing from the traditional egg-based method of flu vaccination generation, a production method common to other vaccines, cell culture, is increasingly gaining currency. Cell-culture technology involves growing key vaccine components in human, monkey, canine, insect, or other cells in enclosed vats. The process has been used for vaccines such as polio, hepatitis A, chickenpox, and shingles, said Robin Robinson, PhD, senior project officer for the Office of Public Health Emergency Preparedness in the US Department of Health and Human Services (HHS). Using traditional methods in the event of an emergency, there is no way to quickly scale up the supply, since the production process takes at least six months. With cell-culture methods, the virus does not need to be adapted for growth in eggs, and in an emergency, manufacturers could boost production by at least a month without waiting for chickens to lay enough eggs. Furthermore, production of cell-culture vaccines is considered safer and cleaner because it uses a closed system of bioreactors. However, a vaccine cannot be specifically tailored to a pandemic virus until the virus emerges, so even with cell-culture technology, a vaccine would not be available for the first several months of a pandemic.

Source: <http://www.cidrap.umn.edu/cidrap/content/influenza/panflu/news/june2705cell.html>

20. *June 27, The Uvalde Leader News (TX)* — **Texas emergency room strives to improve service despite nurse shortage.** In September 2004 the Uvalde Memorial Hospital (UMH) in Uvalde,

TX, added a four-room fast-track area to the emergency department in the hopes of decreasing patient waiting room time. James Buckner Jr., administrator of UMH said that wait times in the ER have been reduced dramatically since last year due to the new fast-track area and increased staff. "It's frustrating to deal with the fact that ten to 20 percent of the time, patients may have to wait for more than two hours...We make our best effort at staffing and try to accommodate staffing for our peak hours," said Buckner. Despite an increase in staff at UMH, there is a nursing shortage; this problem is not just in the Uvalde area but nation wide, according to Buckner. Licensed vocational nurses and registered nurses are highly sought after nationwide. Buckner said that although this is not the first time the hospital has experienced a nursing shortage, "[Lack of] Registered Nurses (RNs) are becoming a critical problem". Currently the hospital has around six nursing positions to be filled, some of which are temporarily being filled by expensive agency nurses, according to Buckner.

Source: http://www.uvaldeleadernews.com/articles/2005/06/27/news/new_s4.txt

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

21. *June 28, Associated Press* — Report on South Carolina train wreck praises local response.

According to a report released Monday, June 27, deputies and state agents in Aiken County, SC, quickly protected a number of sites across the county after a January train wreck in Graniteville just in case the crash and deadly chlorine gas spill were acts of terrorism. The sheriff's office gave itself mostly high marks for responding quickly in the hours after the crash, keeping the site secure and returning evacuees orderly in the days after the crash. The sheriff's report praised the rapid response, aided by gas masks and other equipment officers carried in their cars. The report said deputies did a good job getting news out about the wreck and setting up a safety perimeter around the crash. New radio systems allowed a number of different agencies to communicate easily, according to the report. But a reverse 911 system that calls homes in an area and gives a recorded message was not activated quickly enough because only emergency management employees could access the system. And, in the hours after the crash, the coroner did not have protective equipment to get close to the wreck. The deputies also plan to find better ways to take care of pets left behind.

Source: <http://www.thestate.com/mld/thestate/news/local/12001568.htm>

22. *June 26, Rochester Democrat and Chronicle (NY)* — Students train to support first

responders. Nineteen students from John Marshall High School in Rochester, NY, have graduated from a Community Emergency Response Team (CERT) program sponsored by the Rochester Fire Department. They were the first class of students in the City School District to participate in the CERT program. The students trained three hours a week for eight weeks and learned disaster preparedness, fire chemistry and suppression, treatment of life-threatening conditions, medical care and injury assessment, search and rescue procedures, and

cardiopulmonary resuscitation, among other things. The idea was to train the students so they could provide support to first responders during emergencies in their communities. The 19 students each received community service credit for their work.

Source: <http://www.democratandchronicle.com/apps/pbcs.dll/article?AI=D=/20050626/NEWS01/506260354/1002/NEWS>

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

23. *June 28, Reuters* — **Internet crashes in Pakistan.** An undersea cable carrying data between Pakistan and the outside world has developed a serious fault, virtually crippling data feeds, including the Internet, telecommunications officials said. The system crashed late on Monday, June 27, and was still down on Tuesday evening. Many offices across the country ground to a halt as people realized it was not one of Pakistan's regular, but usually brief, technical hitches. An official at the Karachi stock exchange said Pakistan's main bourse was unaffected as it had its own internal trading system. Fixing it would entail an interruption for other countries using the link, including India, Dubai and Oman, one company official said. But the impact on neighboring countries would be limited and the repairs would begin at 4 a.m. on Wednesday (2300 GMT on Tuesday) to minimize any disruption, he said. Airlines and credit card companies were among the businesses hit by the crash. "It's a total disaster," said Nasir Ali, commercial director of the private Air Blue airline. "We have a Web-based booking system which has totally collapsed."

Source: <http://www.cnn.com/2005/WORLD/asiapcf/06/28/pakistan.internet.reut/index.html>

24. *June 26, Security Focus* — **TCP-IP Datalook Local Denial of Service Vulnerability.** TCP-IP Datalook is affected by a local denial of service vulnerability. Specifically, an attacker can send a specially crafted packet to the listening port of TCP-IP Datalook and cause a crash. TCP-IP Datalook 1.3 is reported to be affected by this issue. Other versions may be vulnerable as well. A vendor-supplied patch is not currently available.

Source: <http://www.securityfocus.com/bid/14061/info>

25. *June 22, Security Focus* — **Veritas Backup Exec Remote Agent for Windows Servers Authentication Buffer Overflow Vulnerability.** VERITAS Backup Exec Remote Agent for Windows Servers is prone to a remotely exploitable buffer overflow vulnerability. This issue occurs when handling authentication requests. Successful exploitation could result in arbitrary code execution. Hotfixes are available from the vendor.

Source: <http://www.securityfocus.com/bid/14022/info>

26. *June 22, Security Focus* — **Veritas Backup Exec Web Administration Console Remote Buffer Overflow Vulnerability.** VERITAS Backup Exec Web Administration Console is prone to a remote buffer overflow vulnerability. An attacker can exploit this issue by crafting a malicious request. This request must contain excessive string data that triggers this issue, replacement memory addresses, and executable instructions. When the Web Administration Console processes this request, the attacker-supplied instructions may be executed on the vulnerable computer. The vendor has released an advisory (VX05-005) and fixes to address

this issue.

Source: <http://www.securityfocus.com/bid/14025/info>

27. May 26, Government Accountability Office — GAO-05-434: Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities (Report).

GAO was asked to determine (1) DHS's roles and responsibilities for cyber critical infrastructure protection, (2) the status and adequacy of DHS's efforts to fulfill these responsibilities, and (3) the challenges DHS faces in fulfilling its cybersecurity responsibilities. DHS established the National Cyber Security Division to take the lead in addressing the cybersecurity of critical infrastructures. While DHS has initiated multiple efforts to fulfill its responsibilities, it has not fully addressed any of the 13 responsibilities, and much work remains ahead. DHS established the US-CERT as a public/private partnership to make cybersecurity a coordinated national efforts. However, DHS has not yet developed national cyber threat and vulnerability assessments or government/industry contingency recovery plans for cybersecurity, including a plan for recovering key Internet functions. DHS faces a number of challenges which include achieving organizational stability, gaining organizational authority, overcoming hiring and contracting issues, increasing awareness about cybersecurity roles and capabilities, establishing effective partnerships with stakeholders, achieving two-way information sharing with these stakeholders, and demonstrating the value DHS can provide. Until it confronts and resolves these underlying challenges and implements its plans, DHS will have difficulty achieving significant results in strengthening the cybersecurity of our critical infrastructures.

Highlights: <http://www.gao.gov/highlights/d05434high.pdf>

Source: <http://www.gao.gov/new.items/d05434.pdf>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT reports VERITAS has released security advisories disclosing vulnerabilities that affect multiple versions of Backup Exec for Windows and Netware Servers. Several components of Backup Exec are affected, including the Remote Agent, Server, NetBackup, Web Administration Console, and Admin Plus Pack Option. For more information, please see http://www.us-cert.gov/current/current_activity.html

The impact of the vulnerabilities ranges from Denial of Service (DoS) conditions to remote execution of arbitrary code. VERITAS has released patches to eliminate all of the reported issues. It is strongly recommended that administrators apply the patches immediately, as historically, vulnerabilities affecting Backup Exec have been targeted by attackers in a widespread fashion.

* http://support.veritas.com/menu_ddProduct_BEWNT_view_ALERT.htm

Updated Port Status: Reports of increased activity on port 6101 have continued.

Activity targeting TCP port 10000 has significantly increased since the release of the

Metasploit Framework module. Administrators are strongly urged to apply the hotfixes as soon as possible. Strict filtering of TCP port 10000 and 6101 is also highly recommended. For specific hotfixes and updates please review the following URLs:

* <http://seer.support.veritas.com/docs/276604.htm/a> *
http://www.metasploit.org/projects/Framework/modules/exploits/backupexec_agent.pm

Current Port Attacks

Top 10 Target Ports	445 (microsoft-ds), 135 (epmap), 27015 (halflife), 1026 (---), 6881 (bittorrent), 139 (netbios-ssn), 1433 (ms-sql-s), 80 (www), 4672 (eMule), 137 (netbios-ns) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	---

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[[Return to top](#)]

General Sector

Nothing to report.

[[Return to top](#)]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

[Homeland Security Advisories and Information Bulletins](#) – DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: <http://www.dhs.gov/dhspublic/display?theme=70>

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983–3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.